

July 30, 2020

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

David J. Bradley, Clerk of Court

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Information associated with KIK username
joe12joe126969 which is stored at premises owned,
maintained, controlled, or operated by MediaLab, Inc.Case No. **3:20-mj-107**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
KIK username: joe12joe126969, more fully described in Attachment A, which is attached and fully incorporated herein.

located in the Central District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached and fully incorporated herein

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC § 2251(a)(e)	Production of Child Pornography
18 USC § 2252A(a)(2)(b)(1)	Distribution of Child Pornography

The application is based on these facts:
Affidavit attached.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 7-30-20

City and state: Houston, Texas


Applicant's signature

Patrick M. York, FBI Special Agent
Printed name and title


Judge's signature

Andrew M. Edison, United States Magistrate Judge
Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

IN THE MATTER OF THE SEARCH OF §
Information associated with Kik User Account §
Joe12Joe126969, which is stored at premises §
owned, maintained, controlled, or operated by §
MediaLab, Inc. §

Case No. **3:20-mj-107**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I. Introduction:

Your Affiant, Patrick M. York, being duly sworn, deposes and says:

A. Introduction and Agent Background:

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) currently assigned to the Houston Division Texas City Residence Agency investigating violent crime matters, which includes crimes against children. I have been a Special Agent of the FBI since February 2009. While in the FBI, I have been assigned to a violent crime squad investigating and assisting with investigations of gangs, drugs, fugitives, crimes against children, and crimes in Indian Country, which include sexual assaults, aggravated assaults, and homicides. Prior to the FBI, I was a Texas Peace Officer for over twelve years.
2. I am charged with the duty of investigating violations of the laws of the United States, collecting evidence in cases in which the United States is or may be a party in interest, and performing other duties imposed by law. During my assignment with the FBI, I have participated in the execution of search warrants for documents and other evidence, including computers and electronic media, in cases involving child pornography and the sexual exploitation of children. I have assisted with investigations involving child pornography and the sexual exploitation of children. I have also attended various FBI training for the investigation and enforcement of federal child pornography laws in which computers are used as the means for receiving, transmitting, and storing child

pornography as defined in Title 18, United States Code, Section 2256.

3. I make this affidavit in support of an application for a search warrant for information associated with the following account: Kik username: Joe12Joe126969 (hereinafter, the "SUBJECT ACCOUNT"), which is stored, maintained, controlled, and administered by MediaLab, Inc. (hereinafter "MediaLab"), an electronic applications developer and holding company headquartered at 1237 7th Street, Santa Monica, California 90401. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab disclose to the government records and other information (including the content of communications) in its possession further described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, government-authorized persons will review that information to locate the items described in Section III of Attachment B.

B. Facts and Circumstances:

4. The statements in this affidavit are based upon my investigation, information provided to your Affiant by Special Agents and Task Force Officers (TFO) of the FBI, public source and business records, and my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of a crime, contraband, fruits of a crime, and other items illegally possessed in violation of Title 18, United States Code, Sections 2251 and 2252A (Certain activities relating to material constituting or containing child pornography), are stored at the premises owned, maintained, controlled, or operated by MediaLab located at 1237 7th Street, Santa Monica, California.
5. The evidence of a crime, contraband, fruits of a crime, and other items illegally possessed in violation of the aforementioned statute include, but are not limited to, visual images depicting minors engaged in sexual activity.

C. Statutory Authority:

6. This investigation concerns alleged violations of Title 18, United States Code, Section 2252A(5)(B), which states

(a) Any person who—

(2) knowingly receives or distributes—

(A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or

(B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

(5) (B) knowingly possesses, or accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. Title 18, United States Code, Section 2256(8) defines "child pornography" as any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where--

(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit

conduct; or,

(C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

8. Title 18, United States Code, Section 2256(2)(A) defines "sexually explicit conduct" as actual or simulated--

(i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

(ii) bestiality;

(iii) masturbation;

(iv) sadistic or masochistic abuse; or

(v) lascivious exhibition of the anus, genitals or pubic area of any person.

D. Social Networking Sites and Kik Messenger Background

9. "Social networking" or "social network service" is a term used to describe applications or websites which focus on establishing networks or relationships among individual users based on interests or activities. These services typically consist of a personal online representation of an individual, often referred to as a profile, a list of other individuals with which a person has interests are allowed to view their profile, and a variety of other capabilities, such as the upload and sharing of images and videos. Newer capabilities allow access to the social networks via mobile devices such as cellular telephones and the upload of real-time information to an individual's profile. Most, if not all, of the social networks are accessible via the Internet and allow a member to contact other members via electronic mail (e-mail), instant messaging, or comments placed directly to a member's profile. Normally, information posted by individuals to their own or another individual's profiles are not vetted for accuracy or content.

10. Kik is an instant messaging application for mobile devices. The app is available on most iOS, Android, and Windows Phone operating systems free of charge. Kik uses a

smartphone's data plan or Wi-Fi to transmit and receive messages. Kik also allows users to share photos, sketches, mobile webpages, and other content. Prior to use, Kik Messenger requires users to register an account with a username and password.

E. Probable Cause and Supporting Determinations:

11. On Monday July 13, 2020, a FBI Washington Field Office (WFO) Task Force Officer, was acting in an undercover (UC) capacity as part of the Metropolitan Police Department-Federal Bureau of Investigation ("MPD-FBI") Child Exploitation Task Force, operating out of a satellite office in Washington, D.C. In that capacity, the UC posted an online bulletin message on a specific social media forum known to the UC as a website where users meet to discuss and trade child pornography and child erotica among other things. This site is forum based and offers users an internal email in which they can communicate with other users. Users can start a conversation thread and title the topic for all users to view. Users can respond to the thread for all users to see.
12. On July 4, 2020, the UC posted an advertisement on this site. This advertisement was refreshed on Friday, July 10, 2020. The advertisement read, "33 yo dad into very dark taboo, looking for other younger moms/dads into same." The UC added his KIK¹ account name to the advertisement.
13. On July 13, 2020, the UC received a private KIK message from a KIK user using the screen name "joe12joe126969" with a display name of "Joe Jen". This user was subsequently identified as Richard Reyes TRIGO. During the course of the chat TRIGO identified himself as a 36 year-old male residing in Texas. TRIGO informed the UC that he was married and had daughters ages 2 and 9. During the course of the chat TRIGO made the following comments regarding his kids, "Love spying on them when they are in the shower". "I want to get a spy cam in the house."
14. During the course of the chat TRIGO stated that he was sexually active with his

¹ KIK is an instant messaging mobile application where one can transmit and receive messages, photos, and videos. Users can communicate privately with other users or in groups.

purported 2 year-old daughter. TRIGO stated that he has performed oral sex on her vagina and anus and has rubbed his penis on her body. TRIGO further stated, "Yes love to cum on their feet even get a little on my finger and put it to mouth" During the course of the chat the TRIGO informed the UC that he had, "pussy pics" of his purported 2 year-old daughter who he later described as being 1 and a half. During the course of the chat the UC informed TRIGO that he was sexually active with his purported 8 year-old daughter. The UC sent TRIGO a clothed image of his purported daughter (not a real child)². TRIGO sent the UC an image of his purported daughter's bare vagina. The picture is a close up shot of what appears to be a toddler's vagina. A male's hand is seen touching the toddler's inner thigh.

15. During the course of the chat TRIGO stated that he met a friend that resides close to him in Texas. TRIGO stated that he has invited this friend over and allowed him to have sexual contact with his minor female relative. TRIGO stated he invites him over when he knows that his wife will be out of the house. During the course of the chat TRIGO stated that he was at work and informed the UC that he would be home at 6pm. TRIGO stated, "Love to show you live pics of her."
16. Also within the chat messages between TRIGO and the UC, TRIGO admitted to having pictures of his minor female relative's vagina. The UC asks TRIGO "what pic do you jerk to most". TRIGO responds with two messages, "Where my cock is to her pu." Then, "Pussy."
17. On July 13, 2020, at approximately 8:08pm EST, TRIGO sent the UC a live camera image of a toddler child. The image depicted the toddler's buttocks from the side and she appeared to be on her knees. A light purple shirt can be seen on the toddler. The UC asked TRIGO if he could hold up 3 fingers near the toddlers head in an attempt to ascertain if TRIGO had immediate access to a real kid. TRIGO complied and sent the UC

² The images the UC sent to TRIGO did not depict a real child.

an image of himself holding up 3 fingers near his child's head. The child is wearing the same purple shirt as described above.

18. During the course of the chat TRIGO stated that he took his child's diaper off and was "playing" with her. TRIGO stated that he was rubbing his penis on his child's vagina and was licking her vagina and anus. TRIGO sent the UC a live camera image of his daughter's bare vagina. The focus of the image is on the child's bare vagina. A male has his fingers on her thigh. The same purple shirt can be seen on the child as described above.
19. On Tuesday, July 14, 2020, the UC continued to communicate with TRIGO. TRIGO sent the UC an image of his purported wife. The picture was that of a clothed Hispanic female. During the course of the chat the UC asked TRIGO about the friend that he allows access to his minor female relative. TRIGO stated, "He plays with my youngest. He puts his dick to her mouth"
20. An emergency disclosure form was submitted to KIK c/o MediaLab requesting subscriber identification and IP logs associated with username joe12joe126969. KIK's response provided display name "Joe Jen", unconfirmed email address remjoe735@gmail.com, device description Samsung android SM-N950U, and IP logs spanning June 15, 2020 through July 14, 2020. Examination of the IP logs yielded a combination of AT&T Wireless, T-Mobile Wireless, and Hughes Network IP addresses.
21. An administrative subpoena was served on Hughes Network requesting subscriber identification and service address information associated with IP address 67.44.192.96 Port 34078 on June 30, 2020 at 18:53:20 UTC. This was the only non-wireless IP address in the logs provided by KIK. Hughes' response identified the subscriber as Maria Fuentes, with a service address of 1507 Airline Court, Rosharon, TX 77583.
22. Upon receipt of this information, FBI Washington used available open source (e.g., Google, Facebook), commercial (e.g., Accurint), and law enforcement sensitive (e.g., NCIC, Texas DMV) databases to fully identify the suspected user of KIK account

joe12joe126969 as Richard Reyes TRIGO (DOB: 12/07/1985). His wife was identified as Ericka Genev Villarreal. A Driver's license photo of Villarreal matched the image that TRIGO sent the UC of his wife. Publicly available photographs on Villarreal's Facebook profile provide an image of a child that appears to be the same age as the child depicted in the illicit photos that TRIGO sent the UC.

23. On July 14, 2020, Affiant requested and obtained a search warrant for 1507 Airline Court, Rosharon, Texas, as well as, an arrest warrant for TRIGO for the production and distribution of child pornography. The search and arrest warrants were issued by United States Magistrate Judge Andrew M. Edison, in the Southern District of Texas.
24. On July 14, 2020 at approximately 9:56 p.m., the search warrant was executed at 1507 Airline Court, Rosharon, Texas. No one was home at the time of the search. During the search, agents observed and seized bed linen matching the description of linen depicted in two of the images sent by TRIGO to the UC on July 13, 2020. The bed linen was found in the bedroom of TRIGO and Villarreal.
25. Agents learned TRIGO was possibly at a different residence in Houston, Texas. On July 15, 2020, at approximately 1:15 a.m., agents located TRIGO at that residence where he was arrested without incident. Also present at the residence were TRIGO's parents, his wife and four minor relatives.
26. During the arrest and subsequent interview with Villarreal at the residence, Villarreal stated to agents that on July 13, 2020, TRIGO was alone with their minor female relatives at their home in Rosharon, Texas, around 6:30 p.m. to 8:00 p.m. when she went to the grocery store. This time frame coincides with the KIK messages between TRIGO and the UC on July 13, 2020 at 20:25 UTC-4 (7:25 p.m. Rosharon, Texas time), where TRIGO informed the UC, "Her mother left shopping so I get to play."
27. TRIGO was interviewed after his arrest. TRIGO was read his Miranda warning and he stated he understood his rights and waived his rights. During questioning, TRIGO admitted to using his cellular phone to access his KIK account and to producing and distributing child pornography from the Device.

28. The FBI is requesting that MediaLab produce records from June 1, 2020 through July 16, 2020. Furthermore, that such records be produced by MediaLab and provided to the FBI within 30 calendar days of receiving service of this court order.

F. Search Procedure for KIK/MediaLab:

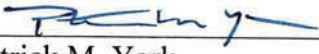
29. In order to facilitate seizure by law enforcement of the records and information described in Attachment B, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of Kik/MediaLab to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:
- a. The search warrant will be presented to Kik/MediaLab personnel, who will be directed to the information described in Section II of Attachment B;
 - b. In order to minimize any disruption of computer service to innocent third parties, Kik/MediaLab employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II of Attachment B, including an exact duplicate of all information stored in the computer accounts and files described therein;
30. Kik/MediaLab employees will provide the exact duplicate in electronic form of the information described in Section II of the Attachment B and all information stored in those accounts and files to the agent who serves this search warrant; and
31. Following the protocol set out in the Addendum to Attachment B, law enforcement personnel will thereafter review all information and records received from Kik/MediaLab employees to locate the information to be seized by law enforcement personnel pursuant to Section III of Attachment B.

G. Conclusion:

32. Based on the forgoing, I request that the Court issue the proposed search warrant. Since the warrant will be served on MediaLab who will then compile the requested records at a

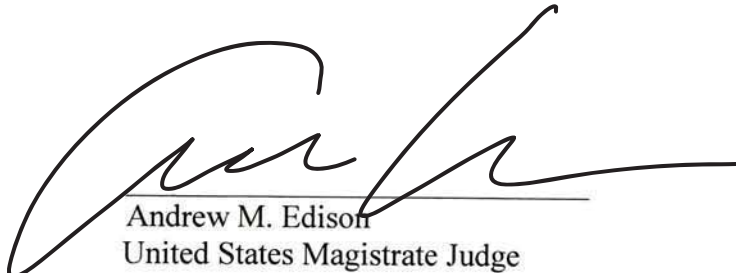
time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

33. This Court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).
34. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of these warrants.



Patrick M. York
Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me telephonically me this 30th day of July 2020, and I find probable cause.



Andrew M. Edison
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

This warrant applies to information associated with the following SUBJECT ACCOUNT identifiers:

Kik username: **joe12joe126969**

This account is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., a company with headquarters at 1237 7th Street, Santa Monica, California 90401.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

The FBI is requesting that MediaLab, Inc. produce records from June 1, 2020 through July 16, 2020. Furthermore, that such records be produced by MediaLab and provided to the FBI within 30 calendar days of receiving service of this court order

I. Search Procedure

1. The search warrant will be presented to MediaLab, Inc. (MediaLab) personnel, who will be directed to isolate those accounts and files described in Section II below.
2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.
3. MediaLab employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant.
4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. Files and Accounts to be Copied by Employees of MediaLab

To the extent that the information described below in Section III is within the possession, custody, or control of MediaLab, they are required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A:

- a. All subscriber information for the SUBJECT ACCOUNT: including full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- b. All media, including all photos, images, and videos created, uploaded, or livestreamed by the SUBJECT ACCOUNT; all Exchangeable Image File (or EXIF) data associated with those photos and videos, including date, time, type of device, and geolocation information; and all photos and videos uploaded by any user that have that user tagged in them.
- c. All contact information, including all Kik Messenger accounts the SUBJECT ACCOUNT contacted, received contact from, or exchanged communications with.
- d. All communications, including instant messages, conversations, chats, and video chats, made or received by the SUBJECT ACCOUNT.
- e. Payments made to or received from other users, including Kin or other cryptocurrency.
- f. All IP logs, including all records of the IP addresses that logged into the SUBJECT ACCOUNT.
- g. The length of service (including start date), the types of service utilized by the SUBJECT ACCOUNT, and the means and source of any payments associated with the service (including any credit card or bank account number).
- h. All privacy settings and other account settings.
- i. All records pertaining to communications between Kik/MediaLab and any person regarding the SUBJECT ACCOUNT or user of the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.
- j. All Kik Messenger/MediaLab accounts associated with the SUBJECT ACCOUNT by cookies, recovery email address, or telephone number.
- k. For the period of time from the creation of the account to the present, any non-content information about the SUBJECT ACCOUNT from companies that are owned or operated by MediaLab.

- l. For the period of time from the creation of the account to the present, any non-content information collected by Kik Messenger/MediaLab about the people and groups the SUBJECT ACCOUNT is connected to, such as the people or groups the SUBJECT ACCOUNT communicates with the most or likes to share with.
- m. For the period of time from the creation of the SUBJECT ACCOUNT to the present, any non-content information shared with vendors, service providers, and other Kik Messenger/MediaLab partners.
- n. For the period of time from the creation of the SUBJECT ACCOUNT to the present, any non-content advertising, measurement and analytical services.
- o. For the period of time from the creation of the SUBJECT ACCOUNT to the present, any information collected by Kik Messenger/MediaLab related to push tokens related to devices associated with the SUBJECT ACCOUNT.
- p. For the period of time from the creation of the account to the present, any information collected by Kik Messenger/MediaLab related to GPS information or any other location information associated with the SUBJECT ACCOUNT.

III. Information to be seized by the government

For the SUBJECT ACCOUNT listed in Attachment A, the search team may seize all information described above in Section II that constitutes evidence, instrumentalities, fruits, and contraband concerning violations of Title 18, United States Code, Sections 2251(a) and (b), and 2252A(a)(1), (2) and (5)(B), including:

1. All information relating to Kik account **joe12joe126969**, including all communications to and from that account from June 1, 2020 through July 16, 2020;
2. Items relating to the use or control of social media accounts and other means of electronic communication, such as email and messaging services;
3. Items relating to communication devices or techniques, including the use of Internet service providers, mobile or cellular phones;
4. Items relating to the identities and current and past physical location of the users of the accounts or the individuals they are communicating with;
5. Items relating to the names, addresses, telephone numbers, email addresses, social media accounts, and other contact or identification information of participants involved in violations of Title 18, United States Code, Sections 2251(a) and (b), and 2252A(a)(1), (2) and (5)(B);
6. All information about payments made to or received from other users, including Kin or other cryptocurrency;
7. All visual depictions, including still images, videos, films, or other recordings, of child pornography as defined in 18 U.S.C. § 2256 or child erotica, including depictions in digital, electronic, documentary, or other form, and any software, hardware, mechanisms, or data used for or capable of being used for the possession, accessing, viewing, receipt, distribution, advertising, or production of the same;
8. All documents, records, communications, correspondence, text messages, instant messages, chats, records of Internet activity, cookies, timestamps, text message logs, instant message logs, and other logs, user profiles, registry information, configuration files, visual depictions, audio recordings or files, and other data or metadata, whether in digital, electronic, documentary, or other form, relating to the following:

- a. The possession, accessing, viewing, receipt, distribution, advertising, or production of child pornography or child erotica, or the attempt to commit these offenses, including data relevant to any person's knowledge or lack of knowledge of these activities and data related to visual depictions described in paragraph 2;
 - b. The identification of persons who used, owned, possessed, or controlled the computers or other items seized and described in the attached affidavit, when and how often they used the items, and what they used the items for;
 - c. The identification or investigation of persons, groups, or online services involved in the possession, accessing, viewing, receipt, distribution, advertising, or production of child pornography or child erotica;
 - d. An interest in child pornography or child erotica, a sexual interest in children under 18, or personal contact and other activities with children;
 - e. Contextual information necessary to understand the evidence described in this attachment.
9. All materials or items that may be sexually arousing to individuals who are sexually interested in minors or that may be used to groom minors for sexual activity, including materials that are not in and of themselves obscene or depicting sexually explicit conduct. These materials or items may include publications and other written materials, children's clothing and toys, "trophy" from children, and photographs, videos, or other depictions of children;
10. All of the non-content records described in Section II.

ADDENDUM TO ATTACHMENT B

With respect to the search of any information and records received from the social network provider, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment B according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;
- b. surveying various file directories and the electronic mail, including attachments thereto to determine whether they include data falling within the list of items to be seized as set forth herein;
- c. opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or;
- d. performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained in such electronic mail, and attachments thereto, exist that are likely to appear in the information to be seized described in Section III of Attachment B.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.